



**KING COUNTY**  
**CHIEF INFORMATION SECURITY/PRIVACY OFFICER**  
**INFORMATION SYSTEMS ANALYST IV**  
**OFFICE OF INFORMATION RESOURCE MANAGEMENT**

**Annual Salary: \$72,427 – \$102,061**

**Job Announcement No.: ESS253**

**OPEN: 2/16/05      CLOSE: Open until filled**

**WHO MAY APPLY:** This position is open to the general public.

**WHERE TO APPLY:** Interested individuals may apply by submitting a current resume, a complete list of five or more personal and professional references, a letter of interest specifically addressing the qualifications listed in this announcement, and the voluntary affirmative action information request, which is attached to this document. Please send all application materials to:

**Stein Stenseng, Executive Search Services - ESS253**

**Voice/Message: (360) 664-1953 E-mail: [steins@dop.wa.gov](mailto:steins@dop.wa.gov)**

**Please make reference to search number ESS253 in the subject line of your E-mail submittal.**

This recruitment is open on an Until Filled basis. The hiring authority reserves the right and may exercise the option to make a hiring decision at any time during the recruitment process, once sufficient qualified candidates are received. Candidate evaluation will be ongoing, and it may be to the applicant's advantage to submit materials expeditiously. Electronic application packages are strongly preferred and must be in MS Word format. King County is an equal opportunity employer. Applicants wishing assistance or alternative formats in the process should contact Youet Heuy at (360) 664-1954, E-mail: [youeth@dop.wa.gov](mailto:youeth@dop.wa.gov), or TDD at (360) 664-6211.

**WORK LOCATION:** 701 Fifth Avenue (Bank of America Tower), Seattle, WA.

**WORK SCHEDULE:** This position is exempt from the provisions of the Fair Labor Standards Act, and is not overtime eligible. The workweek is normally Monday through Friday 8:00 a.m. to 5:00 p.m.

**POSITION PURPOSE:** This is the top security and privacy position at King County. This person will report directly to Chief Information Officer and will oversee and coordinate security and privacy efforts across the organization including information technology, human resources, communications, legal, management and other groups, to identify security and privacy initiatives and standards. The candidate will work closely with the chief information officer, executive management and countywide technology governance and must have working knowledge of information technology. This position requires leadership and will oversee all aspects of information security and privacy; including the security organization where security responsibilities are centralized, decentralized, or matrix managed within the county. This position is responsible for establishing the vision and direction for all information security and privacy projects and programs.

**PRIMARY JOB DUTIES INCLUDE:**

**Security:**

- Direct development of countywide information security policies, standards and guidelines, guide through information technology governance review process, provide agencies guidance on policy implementation, coordinate countywide policy compliance of, and report countywide compliance to CIO.
- Provide advice and consulting to county operational units on matters related to security items such as the security organization, and a network of departmental employees and vendors who safeguard the county's information assets, intellectual property, and computer systems.
- Maintain a library of King County's information security policies, standards and guidelines, both countywide and agency-specific.
- Direct development, refinement and agency use of information security methods and practices, including:

**KING COUNTY IS AN EQUAL OPPORTUNITY EMPLOYER. JOB ANNOUNCEMENTS ARE AVAILABLE IN ALTERNATIVE FORMATS FOR PERSONS WITH DISABILITIES.**

**(206) 296-5209 JOBLINE <http://www.metrokc.gov/ohrm/psd/openings.html> Website Address (206)-296-8535 TTY**

- Incident response methodology
  - Risk management methods
  - Security monitoring and reporting methods and practices
  - Policy compliance methodology
  - Security review and certification practices
- Oversee research of information security tools and direct agency implementation of tools
- Provide advice and consulting to county operational units on matters related to security items such as:
  - Countywide training program
  - Agency corrective actions
  - Risk management activities within agencies
  - Agency incident response activities, and report these to the CIO
  - Agency security monitoring and reporting, and report breaches to the CIO
- Update annual information security advisory management report to the agencies.
- Conduct security reviews and assist in audits as requested by agencies and the CIO.
- Provide research to agencies and the CIO on legal and compliance issues.
- Develop a strategic plan for countywide information security.
- Chair the information technology governance sub team on information security.
- Work with department directors and information technology managers to raise security awareness and integrate security issues into daily operations.

#### **Privacy:**

- Oversee the development, implementation, maintenance and adherence to the County's information privacy policies and standards, and the County's compliance with laws, regulations and industry best practices.
- Provide guidance and assistance to agencies, in coordination with legal staff, on the formulation and implementation of information privacy policies and procedures.
- Perform initial and periodic information privacy risk assessments and ongoing compliance monitoring activities as requested by County management.
- Coordinate with legal staff and County management to ensure that the County uses appropriate privacy and confidentiality consent forms, authorization forms, and information notices and materials.
- Oversee, direct, deliver or ensure delivery of privacy training and orientation to all employees, consultants, contractors, alliances, business associates, and other appropriate third parties.
- Participate in the development, implementation and ongoing compliance monitoring of information privacy requirements and responsibilities in vendor contracts and agreements.
- Serve as the central point of contact to the public on their information privacy concerns with the County and as a consultant on information privacy to County agencies.
- Establish and administer a process for managing and resolving the County's privacy complaints.
- Establish and direct a program for the identification, reporting, and remediation of privacy and information security concerns throughout the organization.
- Chair the information technology governance sub team on information privacy.
- Report to executive board on matters of information security and privacy.
- Other duties as assigned.

#### **QUALIFICATIONS:**

- Bachelor's degree (Masters preferred) in computer science, business administration or related field. Must be able to develop technology and business strategies and have strong oral and written communication skills.
- Experience in the public sector is desirable.
- The successful candidate must have a good working knowledge of business and/or systems analysis.
- Advanced knowledge and demonstrated experience in developing and maintaining information security and privacy policies, standards, guidelines, methods and practices based on industry standards, best practices, tools and techniques.

- Advanced knowledge and demonstrated experience with available information security and privacy products and emerging products.
- Advanced knowledge and demonstrated experience in working with laws and regulations that affect information security.
- Demonstrated experience in managing incident response and security operations.
- Advanced knowledge and demonstrated experience with applicable federal and state laws, regulations, and industry standards on information privacy and public disclosure.
- Demonstrated experience in information privacy assessments and policy compliance.
- Demonstrated experience building and managing relationships at all levels in an organization, from the senior leadership team to the technicians, to achieve consensus among diverse audiences with competing goals and objectives.
- Demonstrated experience in planning and overseeing large and small technology projects.
- Demonstrated experience in information security audit, risk management and policy compliance.
- Strong analytical and problem solving skills that show the ability to define, collect, analyze data, establish facts, draw valid conclusions, and make fact-based decisions.
- Well rounded technology knowledge and demonstrated experience including Microsoft, Novell, Unix/Linux, databases, servers, networks, web, applications, telecommunications.
- Excellent oral and written communication skills that include selling ideas, flexibility and good listening.
- Must be an articulate and persuasive leader who can serve as an effective member of the senior management team and who can communicate security-related concepts to a broad range of technical and non-technical staff.
- Thorough understanding of security regulations such as HIPAA and GLBA are required.
- Thorough understanding of security standards such as ISO 17799, COBIT, and NIST is required.
- Experience dealing with the security challenges and issues confronting a large, departmentally diverse, publicly-facing organization.
- Demonstrated experience balancing individual contributions from team members and cultivating a positive team atmosphere in order to drive success.
- Excellent business management and strategic skills that balance highly technical issues with a successful business model.
- Specific knowledge and experience in the following are required:
  - Ability to apply technical and management knowledge in developing and overseeing agency implementation of countywide information security policies, standards, methods, practices, and tools.
  - Directing, overseeing and strategically guiding an organization's information privacy policies, standards and practices.
  - Ability to apply technical and management knowledge in the development, implementation and administration of a comprehensive information privacy program for a complex organization.

**BACKGROUND/SECURITY CHECK FOR FINALISTS:**

Due to this positions access to highly confidential systems & sensitive data, all finalists must agree to a background check and polygraph conducted by the King County Sheriff's office.

**NECESSARY SPECIAL QUALIFICATIONS:**

Licensing/Certification Requirements CISSP (certified information systems security professional) certification is required.

**SELECTION PROCESS:** Competitive applicants may be invited to participate in an interview. Salary will depend on qualifications.

**UNION REPRESENTATION:** This position is not represented by a union.

## VOLUNTARY APPLICANT PROFILE FORM

To ensure equal employment opportunity, we ask your voluntary cooperation in responding to the questions below. This information will be treated as confidential, and will be available only to authorized personnel. Please review the Affirmative Action definitions at the bottom of the page.

**Please save as a Word document and forward completed form with resume to the recruiter listed in the position announcement or print, fill out completely and fax it to (360) 586-1389.**

|                                    |   |               |
|------------------------------------|---|---------------|
| Name (Last, First, Middle Initial) | Recruitment ESS2523 – King County, Chief Information Security & Privacy Officer | Date of Birth |
|------------------------------------|---|---------------|

1. What race(s) or culture(s) do you consider yourself?

- ☐ Black/African-American (870)  
☐ Caucasian/White (800)  
☐ Asian or Pacific Islander (API)  
    ☐ Chinese (605)      ☐ Vietnamese (619)  
    ☐ Filipino (608)      ☐ Asian Indian (600)  
    ☐ Hawaiian (653)      ☐ Japanese (611)  
    ☐ Korean (612)      ☐ Cambodian (604)  
    ☐ Samoan (655)      ☐ Laotian (613)  
    ☐ Guamanian (600)  
    ☐ Other API, specify: \_\_\_\_\_

☐ American Indian (597) Please identify name of the enrolled or principal tribe: \_\_\_\_\_

- ☐ Eskimo (935)  
☐ Aleut (941)  
☐ Hispanic  
    ☐ Mexican, Mexican      ☐ Puerto Rican (727)  
    ☐ -American (722)      ☐ Cuban (709)  
    ☐ Chicano (705)  
☐ Other Spanish, specify: \_\_\_\_\_  
☐ Other Race, specify: \_\_\_\_\_

If you are more than one race, please also check "Multi-Racial" below and indicate your preference for Affirmative Action purposes.

☐ Multi-Racial, preferences: \_\_\_\_\_

2. Are you ☐ Male ☐ Female

3. Have you ever been active duty in the U.S. Armed Forces? ☐ Yes ☐ No

Dates: \_\_\_\_/\_\_\_\_/\_\_\_\_ to \_\_\_\_/\_\_\_\_/\_\_\_\_

☐ Vietnam Era Veteran

☐ Disabled Veteran (Percent of disability: \_\_\_\_)

4. Do you have a physical, sensory, or mental condition that substantially limits any of your major life functions, such as working, caring for yourself, walking, doing things with your hands, seeing, hearing, speaking, learning?  
☐ Yes ☐ No

I certify that this information is true and accurate to the best of my knowledge.

\_\_\_\_/\_\_\_\_/\_\_\_\_  
Date Signature

### Affirmative Action Definitions

**American Indian or Alaskan Native.** A person with origins in any of the original peoples of North America and who maintains cultural identification through documented tribal affiliation or community recognition.

**Asian or Pacific Islander.** A person with origins in any of the original peoples of the Far East, Southeast Asia, the Indian Korea, Pakistan, the Philippine Republic, and Samoa

**Black/African-American.** A person with origins in any of the Black racial groups of Africa

**Hispanic.** A person of Mexican, Puerto Rican, Cuban, Central or South American, or other Spanish culture or origin regardless of race. For example, persons from Brazil, Guyana, or Surinam Would be classified according to their race and would not necessarily be included in the Hispanic category. This category does not include persons from Portugal, who should be classified according to race.

**White/Caucasian.** A person with origins in any of the original peoples of Europe, North Africa, or the Middle East.

**Disabilities.** For Affirmative Action purposes, people with disabilities are persons with a permanent physical, mental, or sensory impairment, which substantially limits one or more major life activities. Physical, mental, or sensory impairment means: (a) any physiological or neurological disorder or condition, cosmetic disfigurement, or anatomical loss affecting one or more of the body systems or functions; or (b) any mental or psychological disorders such as mental retardation, organic brain syndrome, emotional or mental illness, or any specific learning disability. The impairment must be material rather than slight, and permanent in that it is seldom fully corrected by medical replacement, therapy or surgical means.

**Disabled Veteran.** A person entitled to disability compensation under laws administered by the U.S. Department of Veteran Affairs for disability rated at 30 percent or more, or a person whose discharge or release from active duty was for a disability incurred or aggravated in the line of duty.

**Vietnam-era Veteran.** A person who served on active duty for a period of more than 180 days, any part of which occurred between August 5, 1964, and May 7, 1975, and was discharged or released from duty with other than a dishonorable discharge.